

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-311114

(43)Date of publication of application : 07.11.2000

(51)Int.Cl.

G06F 12/14

(21)Application number : 11-122001

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 28.04.1999

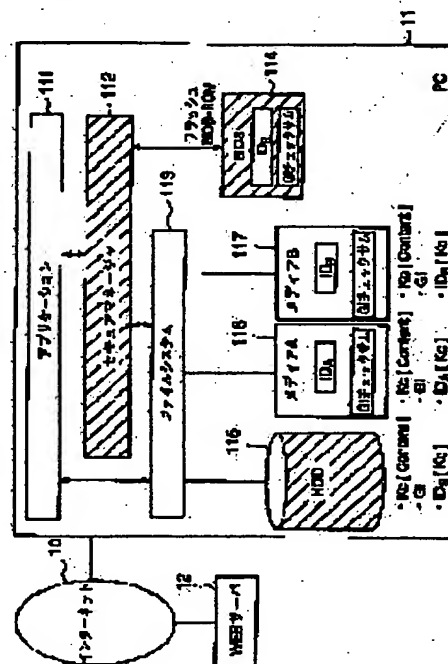
(72)Inventor : ISHIBASHI YASUHIRO
KAMIBAYASHI TATSU
TAMURA MASABUMI

(54) COMPUTER SYSTEM AND CONTENTS PROTECTING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To make compatible the utilization and protection of digital contents by protecting the contents from illegal use even when these contents are recorded on an open recording medium such as hard disk drive.

SOLUTION: When using recording media 116 and 117 having medium ID, a secure manager 112 manages encoding/decoding of contents while using these medium ID. When using an HDD 115 having no medium ID, on the other hand, the secure manager 112 acquires a device ID peculiar to a system through a BIOS and manages encoding/decoding of contents recorded on the HDD 115 while using the device ID. The device ID is stored in a safe area inside a computer system.



LEGAL STATUS

[Date of request for examination]

30.06.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

dec

[Da

dec

[Da

anc

dec

[Da

dec

[Da

er

(11)特許出願公開番号
特開2000-311114
(P2000-311114A)

(43)公開日 平成12年11月7日(2000.11.7)

(51) Int.Cl.⁷
G 0 6 F 12/14

識別記号
320

F I
C O B F 12/14

デーマコート* (参考)

320F 5B017

審査請求 未請求 請求項の数14 O.L (全 10 頁)

(21)出願番号 特願平11-122001

(22) 出願日 平成11年4月28日(1999.4.28)

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

石橋 泰博

(72) 発明者 石橋 泰博

東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

(72) 發明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74) 代理人 100058479

井理士 鈴江 武彦 (外6名)

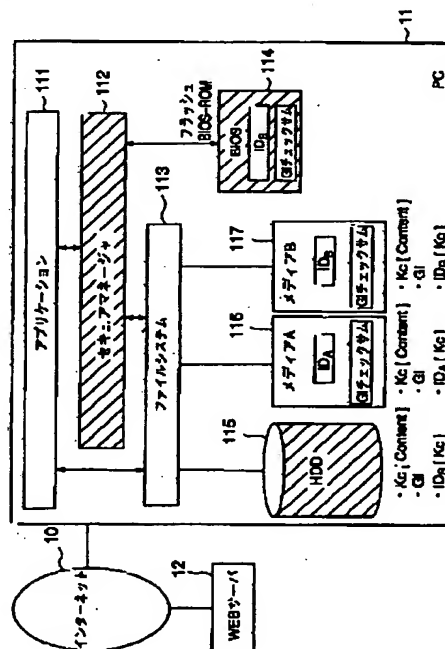
最終頁に続く

(54)【発明の名称】 コンピュータシステムおよびコンテンツ保護方法

(57) 【要約】

【課題】ハードディスクドライブのようなオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようにし、デジタルコンテンツの利用と保護の両立を図る。

【解決手段】セキュアマネージャ112は、メディアIDを有する記録メディア116、117を使用する場合には、コンテンツを記録する記録メディア毎にそのメディアIDを用いてコンテンツの暗号化／復号化の管理を行う。一方、メディアIDを持たないHDD115を使用する場合には、セキュアマネージャ112は、BIOSを介してシステム固有のデバイスIDを取得し、そのデバイスIDを用いて、HDD115に記録するコンテンツの暗号化／復号化を管理する。デバイスIDはコンピュータシステム内の安全な領域に記憶されている。



【特許請求の範囲】

【請求項1】 コンテンツの安全管理のために使用されるデバイスIDを記憶するデバイスID記憶手段と、コンテンツを記録すべき記録メディア毎にその記録メディアが有するメディアIDを用いて前記コンテンツの暗号化／復号化を管理することが可能なコンテンツ管理手段であって、前記メディアIDを持たない記録メディアにコンテンツを記録する場合には、前記デバイスIDを用いて前記コンテンツの暗号化／復号化を管理するコンテンツ管理手段とを具備することを特徴とするコンピュータシステム。

【請求項2】 前記デバイスID記憶手段のデバイスIDは、前記コンピュータシステムのBIOSによって管理されており、

前記コンテンツ管理手段は、前記BIOSとの認証によって、前記デバイスIDを前記BIOSから取得することを特徴とする請求項1記載のコンピュータシステム。

【請求項3】 前記デバイスID記憶手段は前記BIOSを格納するためのBIOS-ROMから構成されており、

前記BIOS-ROMはユーザからはアクセスできない安全な領域を有しており、その領域に前記デバイスIDが格納されていることを特徴とする請求項2記載のコンピュータシステム。

【請求項4】 前記コンテンツにはそのコンテンツの再生／コピー／移動を制限するための制御情報が付加されており、

前記BIOSは前記制御情報の改変検出用のコードデータを管理し、

コンテンツ管理手段は、前記メディアIDを持たない記録メディアに記録されているコンテンツの再生、他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記コンテンツと一緒に前記記録メディアに記録されている前記制御情報と、前記BIOSによって管理されている前記改変検出用コードデータとに基づいて、前記要求された処理の実行を許可または禁止することを特徴とする請求項2記載のコンピュータシステム。

【請求項5】 前記コンテンツ管理手段は、前記メディアIDを持たない記録メディアに記録されているコンテンツを他の記録メディアにコピーする場合には、前記コンテンツのコピー可能回数の値が1減少するように前記メディアIDを持たない記録メディア内の制御情報を更新すると共に、前記メディアIDを持たない記録メディアに記録されているコンテンツと前記更新後の制御情報を前記他の記録メディアにコピーし、且つ更新後の制御情報に基づいて前記BIOSによって管理されている改変検出用コードデータの値を更新することを特徴とする請求項4記載のコンピュータシステム。

【請求項6】 前記コンテンツ管理手段は、前記メディアIDを持たない記録メディアに記録されているコンテンツを他の記録メディアに移動する場合には、前記メディアIDを持たない記録メディアに記録されている制御情報およびコンテンツを前記他の記録メディアに移動した後、前記メディアIDを持たない記録メディアに記録されているコンテンツおよびコピー制御情報を削除することを特徴とする請求項4記載のコンピュータシステム。

【請求項7】 前記コンテンツ管理手段は、前記メディアIDを持たない記録メディアに記録されているコンテンツに対して他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記デバイスIDを用いて前記コンテンツまたはその暗号化鍵の暗号化を解除した後、コピー先または移動先の他の記録メディアのメディアIDを用いて、前記コンテンツまたはそのコンテンツの暗号化鍵を再度暗号化して前記他の記録メディアに記録することを特徴とする請求項5または6記載のコンピュータシステム。

【請求項8】 コンテンツを扱うことが可能なコンピュータシステムにおいて、前記コンテンツの安全管理を行うコンテンツ管理手段を具備し、前記コンテンツ管理手段は、メディアIDを有する記録メディアにコンテンツを記録する場合には、前記メディアIDを用いて前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアIDを有する記録メディアに記録し、メディアIDを持たない記録メディアにコンテンツを記録する場合には、前記コンピュータシステムのBIOSによって管理されている前記コンピュータシステムに固有のデバイスIDを用いて、前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアIDを持たない記録メディアに記録することを特徴とするコンピュータシステム。

【請求項9】 コンピュータシステムのハードウェア制御のためのシステムプログラムを有するコンピュータシステムにおいて、

前記システムプログラムによって管理されている前記コンピュータシステムに固有のデバイスIDを用いて、前記コンピュータシステムの記録メディアに記録すべきコンテンツの暗号化／復号化を管理するコンテンツ管理手段を具備することを特徴とするコンピュータシステム。

【請求項10】 前記コンテンツにはそのコンテンツの再生／コピー／移動を制限するための制御情報が付加されており、

前記システムプログラムは、前記制御情報の改変検出用のコードデータを管理し、前記コンテンツ管理手段は、前記記録メディアに記録されているコンテンツの再生、他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記制御情報の改変検出用のコードデータを管理し、

前記コンテンツ管理手段は、前記記録メディアに記録されているコンテンツの再生、他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記制御情報の改変検出用のコードデータを管理し、

前記コンテンツ管理手段は、前記記録メディアに記録されているコンテンツの再生、他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記制御情報の改変検出用のコードデータを管理し、

き、前記コンテンツと一緒に前記記録メディアに記録されている前記制御情報と、前記システムプログラムによって管理されている前記改変検出用コードデータとに基づいて、前記要求された処理の実行を許可または禁止することを特徴とする請求項9記載のコンピュータシステム。

【請求項11】 コンピュータシステムに固有のデバイスIDを有するコンピュータシステムにおいて、前記コンピュータシステムからデバイスIDを取得し、その取得したデバイスIDを用いて、前記コンピュータシステムの記録メディアに記録すべきコンテンツの暗号化／復号化を管理するコンテンツ管理手段を具備することを特徴とするコンピュータシステム。

【請求項12】 コンテンツを扱うことが可能なコンピュータシステムに適用され、前記コンテンツを不正使用から保護するためのコンテンツ保護方法であって、メディアIDを有する記録メディアにコンテンツを記録する場合には、前記メディアIDを用いて前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアIDを有する記録メディアに記録し、メディアIDを持たない記録メディアにコンテンツを記録する場合には、前記コンピュータシステム内のBIOSによって管理されている前記コンピュータシステムに固有のデバイスIDを用いて、前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアIDを持たない記録メディアに記録することを特徴とするコンテンツ保護方法。

【請求項13】 システム固有のデバイスIDを有するコンピュータシステムで扱われるコンテンツを不正使用から保護するためのコンテンツ保護方法であって、前記コンピュータシステムから前記デバイスIDを取得し、前記取得したデバイスIDを用いて、前記コンピュータシステムの記録メディアに記録すべきコンテンツの暗号化／復号化を管理することを特徴とするコンテンツ保護方法。

【請求項14】 コンピュータシステムで扱われるコンテンツを不正使用から保護するためのコンテンツ保護方法であって、前記コンピュータシステムのハードウェア制御のためのシステムプログラムによって前記コンピュータシステムに固有のデバイスIDを管理しておき、前記システムプログラムから前記デバイスIDを取得し、前記取得したデバイスIDを用いて、前記コンピュータシステムの記録メディアに記録すべきコンテンツの暗号化／復号化を管理することを特徴とするコンテンツ保護方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータシステムおよびそのコンピュータシステムに適用されるコンテンツ保護方法に関する。

【0002】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータが種々開発されている。この種のパーソナルコンピュータは、ネットを通じて画像データや音楽データなどの様々なデジタルコンテンツをダウンロードして使用することができる。

【0003】これらデジタルコンテンツは、MPEG2、MP3といったデジタル符号化技術の採用により、品質を落とすことなくダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【0004】

【発明が解決しようとする課題】しかし、パーソナルコンピュータは基本的にオープンなアーキテクチャを有するシステムであるため、パーソナルコンピュータにおけるデジタルコンテンツの保護は実際上困難である。パーソナルコンピュータ上ではデジタルコンテンツはファイルとして扱われるが、ファイルのコピー／移動は基本的に自由に行うことができるからである。特に、パーソナルコンピュータのストレージデバイスとして使用されるハードディスクドライブについては、その仕様はオープンであり、ハードディスクドライブ上に記録されたデジタルコンテンツの秘匿化を図ることは困難である。このため、インターネットからダウンロードしたデジタルコンテンツを一旦ハードディスクドライブに記録した後は、そのデジタルコンテンツをハードディスクドライブから他のメディアに自由にコピーして使用することができてしまう。

【0005】本発明は上述の事情に鑑みてなされたものであり、ハードディスクドライブのようなオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようにし、デジタルコンテンツの利用と保護の両立を図ることが可能なコンピュータシステムおよびコンテンツ保護方法を提供することを目的とする。

【0006】

【課題を解決するための手段】上述の課題を解決するため、本発明のコンピュータシステムは、コンテンツの安全管理のために使用されるデバイスIDを記憶するデバイスID記憶手段と、コンテンツを記録すべき記録メディア毎にその記録メディアが有するメディアIDを用いて前記コンテンツの暗号化／復号化を管理することが可能なコンテンツ管理手段であって、前記メディアIDを持たない記録メディアにコンテンツを記録する場合には、前記デバイスIDを用いて前記コンテンツの暗号化

／復号化を管理するコンテンツ管理手段とを具備することを特徴とする。

【0007】このコンピュータシステムにおいては、同一記録メディアであれば、その記録メディアを別の機器に移動して使用しても自由な再生が可能となるように、コンテンツは各記録メディア毎に用意されたメディアIDを用いて暗号化して記録される。しかし、ハードディスクドライブのような仕様のオープンな記録メディアの場合には、その記録メディア自体にメディアIDを安全に記録することは出来ない。そこで、本発明では、メディアIDを持たない記録メディアにコンテンツを記録する場合には、コンピュータシステムに固有のデバイスIDを用いて、コンテンツまたはそのコンテンツの暗号化鍵を暗号化して記録するという構成を採用している。デバイスIDをコンピュータシステム内の安全な領域で管理することにより、メディアIDを持たない記録メディアについても、メディアIDを持つ専用の記録メディアを使用する場合と同様に、そこに記録されるコンテンツの保護を図ることができる。

【0008】この場合、デバイスIDはBIOSによって管理し、コンテンツ管理手段は、BIOSとの認証によってデバイスIDを取得するように構成することが好ましい。このようにBIOSとの認証によって初めてデバイスIDを取得できるようにすることにより、デバイスIDをより安全に管理することができる。

【0009】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【0010】図1には、本発明の一実施形態に係るパーソナルコンピュータ(PC)のシステム構成が示されている。このパーソナルコンピュータ(PC)11は、画像データや音楽データなどの各種デジタルコンテンツを扱うことが可能なコンピュータシステムである。このパーソナルコンピュータ(PC)11におけるコンテンツ保護の方法は、コンテンツを記録すべき記録メディア毎にその記録メディアのメディアIDを用いてコンテンツの暗号化／復号化を管理することを前提としている。これは、同一記録メディアであれば、その記録メディアを他のパーソナルコンピュータや電子機器で使用しても再生できるようにするためであり、コンテンツは各記録メディアに用意された専用のメディアIDを用いて暗号化して記録される。メディアIDを用いたコンテンツの暗号化／復号化の管理は、そのための専用のソフトウェアであるセキュアマネージャ112によって実行される。このセキュアマネージャ112はタンバ・レジスタント・ソフトウェアとして実現されている。タンバ・レジスタント・ソフトウェアとは、不正な内部解析や改竄などの攻撃に対して防衛機能を備えるソフトウェアを意味する。

【0011】セキュアマネージャ112は図示のように

アプリケーションプログラム111とファイルシステム113との間に位置し、保護対象のコンテンツについての「記録」、「再生」、「コピー」、「移動」などの各種操作は、セキュアマネージャ112を介して行われる。セキュアマネージャ112によるコンテンツの暗号化／復号化管理は、1)専用のメディアIDを内蔵する記録メディアに対するものと、2)メディアIDを持たない通常の記録メディアに対するものとに、大別される。

【0012】(メディアIDを有する記録メディア)まず、メディアIDを有する記録メディアに対する処理について説明する。

【0013】記録メディア(A)116、および記録メディア(B)117は、それぞれセキュアマネージャ112に対応した専用の記録メディアである。これら記録メディアとしては、パーソナルコンピュータ(PC)11や他の各種電子機器に着脱自在に装着可能なメモリカードなどの各種媒体(SSFDC、フラッシュPCカード、ミニディスク)などを使用することができる。

【0014】記録メディア(A)116には、通常のデータ記憶領域の他、その記録メディアに固有のメディアID(ID_A)が予め記憶されているROM領域と、後述のGI(Governance Information)テーブルから作成されたGIチェックサムデータを格納するためのGIチェックサム領域とが設けられている。記録メディア(B)117についても同様の構成である。メディアIDは各記録メディアに固有であれば良く、シリアル番号や製造番号、他の様々な識別情報を利用することができる。

【0015】GIテーブルとは、保護対象の各コンテンツ毎にその再生、コピー、移動の可否、およびコピー可能回数、移動可能回数などを規定したコピー制御情報である。GIチェックサムデータはGIテーブルの内容の改竄を検出するための改変検出用コードデータであり、GIテーブルの値から算出される。GIチェックサムデータの代わりにGIテーブルのハッシュ値を用いることもできる。GIテーブルの「コピー可能回数」の値は、コピーが実行される度に-1減算される。このようにGIテーブルの値が更新される度に、その更新に合わせて、GIチェックサムデータの値も更新される。このため、GIチェックサム領域は書き換え可能な領域から構成されている。

【0016】ROM領域およびGIチェックサム領域のどちらも、ユーザからはアクセスできないセキュアな領域となっている。

【0017】コンテンツを記録メディア(A)116に記録する場合には、セキュアマネージャ112は、記録メディア(A)116のメディアIDを用いてコンテンツの暗号化／復号化を管理する。この場合、記録メディア(A)116のデータ領域には、以下のデータが格納

される。

【0018】・Kc[Content]: コンテンツキーKcと称される秘密鍵によって暗号化されたコンテンツ

・GI

・ID_A[Kc]: 記録メディア(A)116のメディアID(ID_A)によって暗号化されたコンテンツキー

記録メディア(A)116に記録されたコンテンツを再生する場合には、セキュアマネージャ112は、まず、記録メディア(A)116のメディアID(ID_A)を用いてID_A[Kc]を復号化し、Kcを得る。そして、そのKcによって、Kc[Content]を復号化する。

【0019】記録メディア(A)116に記録されたコンテンツがコピー可能なコンテンツである場合、そのコンテンツを記録メディア(A)116から他の記録メディア(例えば記録メディア(B)117)にコピーすることができる。この場合、セキュアマネージャ112は、記録メディア(A)116に格納されたGIからチェックサムデータを生成し、そのチェックサムデータを、記録メディア(A)116のGIチェックサム領域のGIチェックサムデータと比較する。不一致の場合には、コピーは禁止される。一致した場合には、セキュアマネージャ112は、記録メディア(A)116のメディアID(ID_A)を用いてID_A[Kc]を復号化し、Kcを得る。次いで、セキュアマネージャ112は、コピー先の記録メディア(B)117のメディアID(ID_B)を用いてKcを暗号化し、暗号化したコンテンツキー(ID_B[Kc])を、Kc[Content]およびGIと一緒に、記録メディア(B)117のデータ領域に書き込む。この場合、記録メディア(A)116、記録メディア(B)117のどちらにおいても、GIによって指定されるコピー可能回数の値は-1される。例えば、コピーしたコンテンツが「一回のみコピー可」のコンテンツであった場合には、「これ以上コピー不可」のコンテンツに変更される。また、GIの更新に伴い、記録メディア(A)116、記録メディア(B)117それぞれのGIチェックサムデータの値も更新される。

【0020】記録メディア(A)116に記録されたコンテンツが移動可能なコンテンツである場合、そのコンテンツを記録メディア(A)116から他の記録メディア(例えば記録メディア(B)117)に移動することができる。この場合、セキュアマネージャ112は、記録メディア(A)116に格納されたGIからチェックサムデータを生成し、そのチェックサムデータを、記録メディア(A)116のGIチェックサム領域のGIチェックサムデータと比較する。不一致の場合には、移動は禁止される。一致した場合には、セキュアマネージャ

112は、記録メディア(A)116のメディアID(ID_A)を用いてID_A[Kc]を復号化し、Kcを得る。次いで、セキュアマネージャ112は、移動先の記録メディア(B)117のメディアID(ID_B)を用いてKcを暗号化し、暗号化したコンテンツキー(ID_B[Kc])を、Kc[Content]およびGIと一緒に、記録メディア(B)117のデータ領域に書き込む。この後、セキュアマネージャ112は、移動元の記録メディア(A)116のデータ領域に格納されているKc[Content]、GI、ID_A[Kc]を削除すると共に、GIチェックサム領域のGIチェックサムデータを削除する。GIによって規定されているのが「コピー可能回数」のみで、「移動可能回数」については規定されていない場合には、移動によるGIの更新は行われない。「移動可能回数」が規定されている場合には、前述の「コピー」の場合と同様にして、GIは更新された後に記録メディア(B)117に書き込まれ、またその更新後のGIに対応するチェックサムデータがGIチェックサム領域に書き込まれることになる。

【0021】(メディアIDを持たない記録メディア)
次に、メディアIDを持たない記録メディアに対する処理について説明する。HDD115はパーソナルコンピュータ(PC)11の二次記憶装置として使用されるストレージデバイスであり、パーソナルコンピュータ(PC)11に固定されて使用される。HDD115には、記録メディア(A)116、および記録メディア(B)117のようなROM領域やGIチェックサム領域は設けられていない。

【0022】HDD115を用いてコンテンツの記録、コピー、移動などを行う場合、セキュアマネージャ112は、メディアIDの代わりに、本パーソナルコンピュータ(PC)11に固有のデバイスIDを用いて、コンテンツの暗号化/復号化の管理を行う。つまり、セキュアマネージャ112は、コンテンツの記録先、コピー先、コピー元、移動先、または移動元がHDD115に対応するドライブ番号であった場合には、メディアIDではなく、システム内で管理されているデバイスIDを使用する。この場合、どのドライブ番号の記録メディアがメディアIDを持ち、どのドライブ番号の記録メディアがメディアIDを持たないかは、例えば、プラグアンドプレイ等の機能を利用することにより、セキュアマネージャ112がメディア毎に認識できるようにすることもできる。

【0023】PC11固有のデバイスIDは、PC11のハードウェア制御のためのシステムプログラムであるBIOSによって管理されている。BIOSは、そのBIOS自体のアップデートに対応するために、書き換え可能な不揮発性メモリから構成されたフラッシュBIOS-ROM114に格納されている。フラッシュBIOS-ROM114はユーザからはアクセスできないセキ

ユーザ領域を有しており、そこには、図2に示すように、パスワードエリアに加え、IDエリア、チェックサムエリアなどが設けられている。パスワードエリアは、ユーザによって登録されたパスワードを記憶するための領域である。パスワードが登録されている場合には、電源投入時にユーザからの入力パスワードと登録パスワードとの一致の有無が判定され、一致した場合にのみ、OSのブートや、サスペンド/ハイバネーション状態からの復帰が可能となる。

【0024】IDエリアには、PC11に固有のデバイスID (ID_S) が予め記憶されている。チェックサムエリアは、HDD115に記憶されるコンテンツのGIから作成されたGIチェックサムデータの格納に用いられる。

【0025】BIOSには、セキュアマネージャ112との間で認証処理を行うための認証機能が設けられている。セキュアマネージャ112とBIOSとの認証処理により、互いに正しいプログラム同士であることが確認されると、セキュアマネージャ112は、BIOSからデバイスID (ID_S) を取得することができる。このようにBIOSとの認証によって初めてデバイスIDを取得できるようにすることにより、デバイスIDをより安全に管理することができる。

【0026】次に、図3および図5を参照して、HDD115を使用する場合のコンテンツ管理処理の手順について具体的に説明する。

【0027】「記録」図3はコンテンツ記録時の動作の流れを示している。

【0028】(ステップ1)： PC11の起動時には、まず、セキュアマネージャ112とBIOSとの間で認証処理が実行される。互いに正しいプログラム同士であることが確認されると、セキュアマネージャ112とBIOSとの間でキー交換が行われ、同一の認証鍵 (K_{x2}) が共有される。認証鍵 (K_{x2}) は、毎回代わる時変キーである。

【0029】(ステップ2)： セキュアマネージャ112は、ID取得要求をBIOSに発行する。セキュアマネージャ112からのID取得要求に回答して、BIOSは、デバイスID (ID_S) を認証鍵 (K_{x2}) で暗号化し、暗号化されたデバイスID (K_{x2} [ID_S]) をセキュアマネージャ112に送信する。セキュアマネージャ112は、認証鍵 (K_{x2}) を保持しているので、K_{x2} [ID_S] からID_S を解読することができる。

【0030】(ステップ3)： WEBブラウザなどのアプリケーションプログラムを用いてWEBサーバから画像データや音楽データなどのコンテンツをダウンロードする場合には、WEBブラウザを介して、あるいは直接、セキュアマネージャ112とWEBサーバ12との間で認証処理が行われる。互いに正しいコンテンツ保護機能を有するもの同士であることが確認されると、セキュア

マネージャ112とWEBサーバ12との間でキー交換が行われ、同一の認証鍵 (K_{x1}) が共有される。認証鍵 (K_{x1}) は毎回代わる時変キーである。

【0031】(ステップ4)： WEBサーバ12は、要求されたコンテンツを所定のコンテンツキーK_cで暗号化したもの (K_c [Content]) と、認証鍵 (K_{x1}) で暗号化したコンテンツキー (K_{x1} [K_c]) と、GIとを、PC11宛に送信する。

【0032】(ステップ5)： これら、K_c [Content]、K_{x1} [K_c]、GIは、WEBブラウザなどを介して、セキュアマネージャ112に送られる。セキュアマネージャ112は、WEBブラウザから指定されたダウンロード先の記録メディアがHDD115である場合、認証鍵 (K_{x1}) と、BIOSから取得したデバイスID (ID_S) を用いて、K_{x1} [K_c] をID_S [K_c] に変換する。この場合、まず、認証鍵 (K_{x1}) を用いてK_{x1} [K_c] がK_cに復号化され、そのK_cがあらためてID_Sによって暗号化される。

【0033】この後、セキュアマネージャ112は、K_c [Content]、ID_S [K_c]、GIをファイルシステム113、さらにはIDEドライブなどを通して、HDD115に書き込む。

【0034】(ステップ6)： セキュアマネージャ112は、GIからGIチェックサムデータ (GI_CS) を算出し、それをBIOSとの認証鍵 (K_{x2}) で暗号化してBIOSに渡す。BIOSは、GIチェックサムデータを暗号化されたまま、あるいは復号化した後に、フラッシュBIOS_ROM114のチェックサムエリアに書き込む。もちろん、セキュアマネージャ112が直接フラッシュBIOS_ROM114のチェックサムエリアに、GIチェックサムデータあるいはその暗号化データを書き込むようにしても良い。

【0035】「再生」図4はコンテンツ再生時の動作の流れを示している。

【0036】(ステップ1)： PC11の起動時には、まず、セキュアマネージャ112とBIOSとの間で認証処理が実行される。互いに正しいプログラム同士であることが確認されると、セキュアマネージャ112とBIOSとの間でキー交換処理が行われ、同一の認証鍵 (ここでは、K_{x1}とする) が共有される。認証鍵 (K_{x1}) は毎回代わる時変キーである。

【0037】(ステップ2)： セキュアマネージャ112からのID取得要求に回答して、BIOSは、デバイスID (ID_S) を認証鍵 (K_{x1}) で暗号化し、暗号化されたデバイスID (K_{x1} [ID_S]) をセキュアマネージャ112に送信する。セキュアマネージャ112は、認証鍵 (K_{x1}) を保持しているので、K_{x1} [ID_S] からID_S を解読することができる。

【0038】(ステップ3)： 次に、セキュアマネージャ112からのGIチェックサムデータの取得要求に

応答して、BIOSは、GIチェックサムデータ (GI_CS) を認証鍵 (K_{x1}) で暗号化し、暗号化されたGIチェックサムデータ ($K_{x1} [GI_CS]$) をセキュアマネージャ112に送信する。セキュアマネージャ112は、認証鍵 (K_{x1}) を保持しているので、 $K_{x1} [GI_CS]$ からGI_CSを解読することができる。

【0039】(ステップ4)：セキュアマネージャ112は、アプリケーションプログラム111などから指定された再生対象の暗号化されたコンテンツ ($Kc [Content]$) と、それに対応するID_s [Kc]、およびGIを、ファイルシステム113、さらにはIDEドライバなどを介して、HDD115から取得する。

【0040】(ステップ5)：セキュアマネージャ112は、GIからチェックサムを算出し、その算出したチェックサムと、BIOSから取得したGI_CSとを比較する。不一致の場合には、HDD115のGIが悪意を持つユーザによって書き替えられた恐れがあるため、再生処理はこの時点で中止する。一致した場合には、セキュアマネージャ112は、BIOSから取得したID_s を用いて、ID_s [Kc] を復号し、 Kc を得る。そして、その Kc を用いて $Kc [Content]$ の暗号を解除し、生のコンテンツ (Content) を再生ソフト (プレイヤ) に送信する。再生ソフトもタンバ・レジスタント・ソフトウェアとして実現されている。

【0041】「コピー」図5はコンテンツコピー時の動作の流れを示している。ここでは、HDD115に記録されているコンテンツを記録メディア(A)116にコピーする場合を例示する。

【0042】(ステップ1)：PC11の起動時には、まず、セキュアマネージャ112とBIOSとの間で認証処理が実行される。互いに正しいプログラム同士であることが確認されると、セキュアマネージャ112とBIOSとの間でキー交換処理が行われ、同一の認証鍵 (ここでは、 K_{x1} とする) が共有される。認証鍵 (K_{x1}) は毎回代わる時変キーである。

【0043】(ステップ2)：セキュアマネージャ112からのID取得要求に応答して、BIOSは、デバイスID (ID_s) を認証鍵 (K_{x1}) で暗号化し、暗号化されたデバイスID ($K_{x1} [ID_s]$) をセキュアマネージャ112に送信する。セキュアマネージャ112は、認証鍵 (K_{x1}) を保持しているので、 $K_{x1} [ID_s]$ からID_s を解読することができる。

【0044】(ステップ3)：次に、セキュアマネージャ112からのGIチェックサムデータの取得要求に応答して、BIOSは、GIチェックサムデータ (GI_CS) を認証鍵 (K_{x1}) で暗号化し、暗号化されたGIチェックサムデータ ($K_{x1} [GI_CS]$) をセキュアマネージャ112に送信する。セキュアマネージャ1

12は、認証鍵 (K_{x1}) を保持しているので、 $K_{x1} [GI_CS]$ からGI_CSを解読することができる。

【0045】(ステップ4)：セキュアマネージャ112は、アプリケーションプログラム111などから指定されたコピー対象の暗号化されたコンテンツ ($Kc [Content]$) と、それに対応するID_s [Kc]、およびGIを、ファイルシステム113、さらにはIDEドライバなどを介して、HDD115から取得する。

【0046】セキュアマネージャ112は、GIからチェックサムを算出し、その算出したチェックサムと、BIOSから取得したGI_CSとを比較する。不一致の場合には、HDD115のGIが悪意を持つユーザによって書き替えられた恐れがあるため、コピー処理はこの時点で中止する。一致した場合には、HDD115のGIを参照して、コピー対象のコンテンツがコピー可能なコンテンツであるか否かを調べる。「コピー不可」または「コピー可能回数=零」の場合には、コピー処理はこの時点で中止する。コピーが許されたコンテンツであれば、セキュアマネージャ112は、次のステップ5以降の処理に進む。

【0047】(ステップ5)：セキュアマネージャ112は、コピー先の記録メディア(A)116またはそれを制御するためのデバイスドライバとの間で認証処理を行う。互いに正しいコンテンツ保護機能をもつもの同士であることが確認されると、セキュアマネージャ112とコピー先の記録メディア(A)116またはそのデバイスドライバとの間でキー交換が行われ、同一の認証鍵 (ここでは、 K_{x2} とする) が共有される。認証鍵 (K_{x2}) は毎回代わる時変キーである。

【0048】(ステップ6)：セキュアマネージャ112からのID取得要求に応答して、記録メディア(A)116またはそのデバイスドライバは、メディアID (ID_a) を認証鍵 (K_{x2}) で暗号化し、暗号化されたメディアID ($K_{x2} [ID_a]$) をセキュアマネージャ112に送信する。セキュアマネージャ112は、認証鍵 (K_{x2}) を保持しているので、 $K_{x2} [ID_a]$ からID_a を解読することができる。

【0049】(ステップ7)：セキュアマネージャ112は、HDD115から取得したGIを更新し、「コピー可能回数」が-1されたGI' を得る。そして、BIOSから取得したデバイスID (ID_s) を用いてID_s [Kc] を復号化し、 Kc を得る。次いで、セキュアマネージャ112は、 Kc をメディアID_a を用いて暗号化し、ID_a [Kc] を得る。この後、セキュアマネージャ112は、 $Kc [Content]$ 、ID_a [Kc]、GI' を、ファイルシステム113さらには記録メディア(A)116のドライバなどを介して記録メディア(A)116に書き込む。

【0050】(ステップ8)：セキュアマネージャ1

12は、GI' からそのチェックサムデータ (GI' _CS) を算出し、それを認証鍵 (K_{x2}) で暗号化したもの (K_{x2} [GI' _CS]) を記録メディア (A) 116またはそのドライブに送信し、GI' _CSを記録メディア (A) 116のGIチェックサム領域に書き込む。

【0051】(ステップ9): この後、セキュアマネージャ112は、チェックサムデータ (GI' _CS) をBIOSとの認証鍵 (K_{x1}) で暗号化し、それをBIOSに送信する。BIOSは、フラッシュBIOS_ROM114のチェックサムエリアの内容をGI' _CSに書き替える。

【0052】(ステップ10): そして、セキュアマネージャ112は、HDD115のGIをGI' に更新する。

【0053】「移動」HDD115に記録されているコンテンツを記録メディア (A) 116に移動する場合は、図5のコピー処理と基本的に同じ手順で処理が行われるが、ステップ9の代わりにフラッシュBIOS_ROM114のチェックサムエリアの内容を削除する処理が行われ、また図5のステップ10の代わりにHDD115のKc [Content]、ID_s [Kc]、およびGIを削除する処理が行われる、点がコピー処理とは異なる。また、移動の場合は、コピー可能回数に対するGIの更新は行われず、移動可能回数が規定されている場合を除き、GIは更新されずに移動先の記録メディア (A) 116に書き込まれることになる。

【0054】以上のように、本実施形態においては、BIOSにセキュアマネージャ112との認証機能やデバイスID管理機能を持たせることにより、メディアIDを持たない記録メディアにコンテンツを記録する場合でも、メディアIDを持つ専用の記録メディアを使用する場合と同様に、そこに記録されるコンテンツの保護を図ることができる。特に、デバイスIDおよびGIチェックサムデータをBIOSによって管理し、システム側からはアクセスできないようにしているので、HDD115に対して何ら変更を加えることなく、HDD115にダウンロードしたコンテンツを不正使用から保護することができる。

【0055】なお、本実施形態では、コンテンツの暗号化鍵であるコンテンツキーをメディアIDやデバイスIDを用いて暗号化するようにしてが、メディアIDやデバイスIDをコンテンツキーとして使用し、コンテンツ自体をメディアIDやデバイスIDを用いて暗号化するようにしてもよい。また、メディアIDを持たない記憶メディアとしてHDDを例示したが、デバイスIDを用いて暗号化/復号化の管理を行う本実施形態のコンテンツ保護方法は、例えば、MOやメモ리카ードなど、メディアIDを持たない通常の記憶メディア全てに対して適用することができる。

【0056】また、デバイスIDはPC11内の安全な記憶装置に記憶してあればよく、例えば、PC11内の埋め込みコントローラ (EC) 内に記憶したり、PC11内に設けられているリアルタイムクロック内のバッテリバックアップされたCMOSメモリなどに記憶してもよい。PC11内のどこにデバイスIDを記憶した場合でも、BIOSを介してデバイスIDを取得するようにすることにより、セキュアマネージャ112はデバイスIDの記憶場所を意識することなく、必要な処理を行うことができる。

【0057】さらに、本実施形態は、PCに限らず、セットトップボックス、ゲーム機、オーディオ/ビデオプレーヤーなど、マイクロプロセッサを搭載したあらゆるデータ処理装置 (コンピュータ応用機器) に適用することができる。

【0058】また、セキュアマネージャ112の機能、つまり、前述したようにBIOSからデバイスIDを取得し、そのデバイスIDを用いてコンテンツの暗号化/復号化を管理する手順や、メディアIDを有する記録メディアについてはそのメディアIDを用いてコンテンツの暗号化/復号化を管理する手順などを含むコンピュータプログラムを通信媒体や記録媒体を介してコンピュータに導入することにより、BIOSによってデバイスIDを管理することが可能なシステムであれば、本実施形態と同様の効果を得ることができる。また、BIOSについても、そのアップデートが可能であるので、通常のハードウェア制御機能に加え、認証機能や、デバイスIDおよびその管理機能などを持つ新たなBIOSを通信媒体や記録媒体を介してコンピュータに導入すれば、既存のコンピュータにおいても本実施形態と同様の効果を得ることができる。

【0059】

【発明の効果】以上説明したように、本発明によれば、ハードディスクドライブのようなオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようになり、デジタルコンテンツの利用と保護の両立を図ることが可能となる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンピュータシステムの基本構成を示すブロック図。

【図2】同実施形態のコンピュータシステムに設けられたフラッシュBIOS_ROMの記憶内容の一例を示す図。

【図3】同実施形態のコンピュータシステムで行われるコンテンツ記録処理の手順を示す図。

【図4】同実施形態のコンピュータシステムで行われるコンテンツ再生処理の手順を示す図。

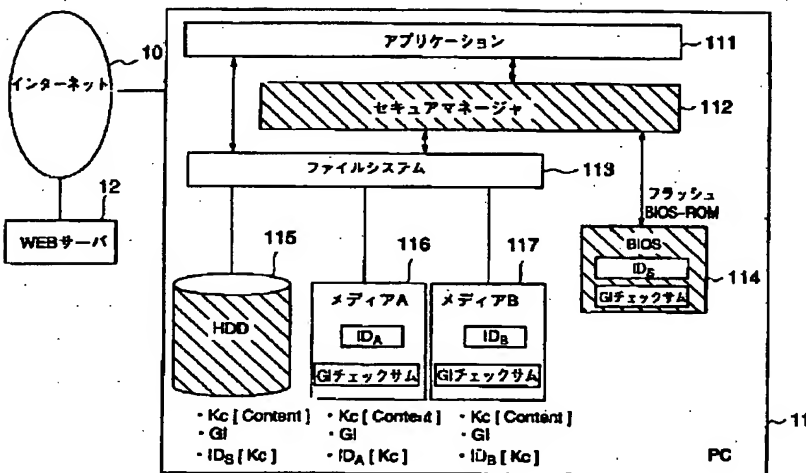
【図5】同実施形態のコンピュータシステムで行われるコンテンツコピー処理の手順を示す図。

【符号の説明】

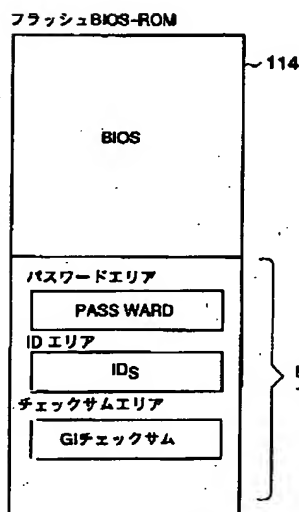
10…インターネット
 11…パーソナルコンピュータ (PC)
 12…WEBサーバ
 111…アプリケーションプログラム
 112…セキュアマネージャ

113…ファイルシステム
 114…フラッシュBIOS_ROM
 115…HDD
 116…記録メディア (A)
 117…記録メディア (B)

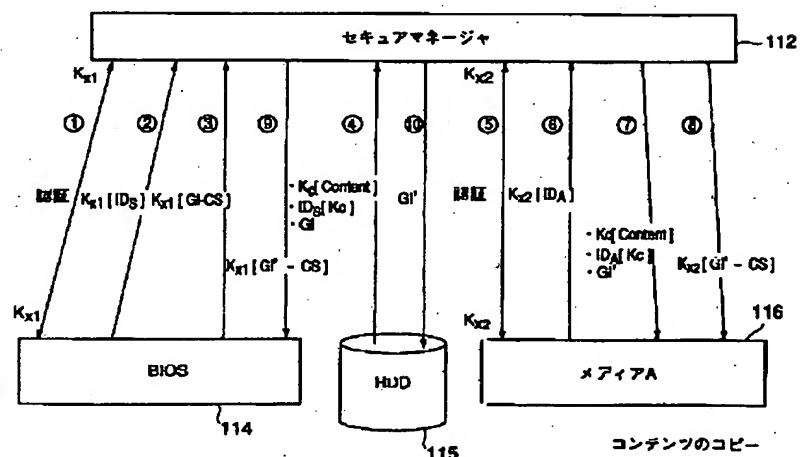
【図1】



【図2】



【図5】





Fターム(参考) 5B017 AA06 AA07 BA07 BB06 BB10
CA16